

Applicant: Stein et al.
For: ADVANCED ENCRYPTION STANDARD (AES) ENGINE WITH
REAL TIME S-BOX GENERATION

5

ABSTRACT OF DISCLOSURE

An advanced encryption standard (AES) engine with real time S-box generation includes a Galois field multiplier system in a first mode responsive to a first data block for generating an AES selection (S-box) function by executing the multiplicative increase in $GF^1(2^m)$ and applying an affine over $GF(2)$ transformation to obtain a subbyte transformation; and a shift register system for transforming the subbyte transformation to obtain a shift row transformation; the Galois field multiplier system is responsive in a second mode to the shift row transformation to obtain a mix column transformation and add a round key for generating in real time an advanced encryption standard cipher function of the first data block.